Remarks

Claims 1, 2, 4, 5, and 7-18 remain in the application. Claims 3 and 6 have been canceled. Claims 1, 4, 7, 8, 10, and 14 have been amended.

Information Disclosure Statement

Re Item 1:

The listing of references in paragraph [009] of the specification has been incorporated by reference through a clerical error. The references referred to in paragraph [009] but not cited in the Information Disclosure Statement relate to background references of general interest but are not considered relevant with respect to the present invention. Applicant has amended paragraph [009] of the specification in order to remove the "incorporation by reference". The amendment does not add new subject matter.

Re Item 2:

Applicant would like to apologize for omitting to provide an explanation of the relevance of German Patent DE 19837642.

Reference DE 19837642 teaches a method and array for controlling an apparatus by means of fingerprint information. The apparatus is controlled depending on fingerprint information provided a user. The fingerprint information is compared with stored fingerprint information pertaining to different fingers of a person, each of which is assigned a different control procedure. Applicant does not consider this reference being pertinent to the present invention as claimed, but as a state of the art example of using different fingerprint information for enabling different control procedures. Applicant

respectfully submits that the present invention as claimed is neither anticipated by this reference nor obvious in light of this reference and other references cited.

Claims

Claims 1, 7, 8, and 10 have been amended in order to avoid invoking 35 U.S.C. 112, sixth paragraph. In particular, all instances of phrases such as --the steps of--, and --the step of-- have been deleted. Applicant wishes to note for the record that the amendments are not intended to be narrowing, nor are the amendments being made for a reason related substantially to patentability. Applicant respectfully submits that no new matter has been added in the amendments.

Claims Rejections – 35 USC § 102

Claims 1-4 are rejected under 35 U.S.C. 102(e) as being anticipated by Matyas Jr. et al U.S. Patent No 6,697,947.

Referring to amended claim 1, Applicant discloses and claims a method for providing access to a secure entity or service by M designated persons having only limited access privileges defined by the following features (emphasis added):

storing biometric data in dependence upon a biometric characteristic of each of the M designated persons;

capturing biometric information representative of a biometric characteristic of each of N persons and providing biometric data in dependence thereupon, **with $1 < N < M$ being a subset of a plurality of predetermined subsets of the M designated persons, wherein some of the subsets of the plurality of predetermined subsets have different access privileges to the secure entity or service;**

comparing the captured biometric data of each of the N persons with the stored biometric data to produce N comparison results; and,

if the N comparison results are indicative of the N persons each being one of the M designated

persons and thereby forming the subset, determining the access privileges to the secure entity or service in dependence upon the subset.

The highlighted features in the method defined in amended claim 1 enables different levels of access to the secure entity or service to different groups of persons – predetermined subsets – of M designated persons in dependence upon the biometric information received. For example, considering two subsets of M=6 designated persons A to F having access privileges to the secure entity or service, with a first subset comprising persons A, B, and C, and a second subset comprising persons D, E, and F. The method as disclosed and claimed enables a first level of access when the received biometric information is indicative of the persons belonging to the first subset, i.e. persons A, B, and C, and a second level of access when the received biometric information is indicative of the persons belonging to the second subset, i.e. persons D, E, and F. However, access to the first level is denied for the second subset and vice versa. Furthermore, access is denied if, for example, the received biometric information is indicative of persons B, D, and E, i.e. if the identified persons do not belong to a predetermined subset – subset 1 or subset 2. In a practical application different groups of bank employees – subset 1 and subset 2 - have limited access to a bank vault to perform certain tasks. For example bank employees belonging to subset 1 have first level access privileges for accessing customers safety deposit boxes while bank employees belonging to subset 2 have second level access privileges for accessing storage rooms for gold and money. This feature ensures that only subsets of bank employees assigned to the tasks in a predefined section are able to access the same. As is evident, the method as defined in amended claim 1 is highly beneficial in numerous applications by substantially increasing security while simultaneously providing flexibility in enabling access to a secure entity or service.

Cited reference Matyas Jr. et al. teaches biometric based multi-party authentication. However, the cited reference does not teach anything similar to the highly advantageous features as highlighted above. In particular, in col. 9 lines 11-14 and lines 24-28, and in col. 10 lines 9-13, reference Matyas teaches only "*It is then determined if the count of valid*

users exceeds the threshold for authentication. ... If the threshold has been reached, then an indication of authenticity is provided." As is evident, the teachings of Matyas Jr. et al. enable access to the secure entity or service when the biometric information is indicative of a predetermined number of designated persons. Considering again the above example, these teachings do not enable access to a first subset and a second subset of the M designated persons but enables access to any combination of designated persons when the biometric information is indicative of a sufficient number of designated persons such as persons B, D, and E. Furthermore, the teachings of Matyas Jr. et al. would enable access to all sections of the bank vault when the biometric information is indicative of persons B, D, and E.

Applicant respectfully submits that the method for providing access to a secure entity or service as defined in claim 1 is highly inventive and not anticipated by Matyas Jr. et al.

The features added in the amendment of claim 1 have been defined in the originally filed dependent claims 3 and 6. Therefore, no new subject matter has been added.

Applicant would like to note that, with regard to Examiner's objection of dependent claim 6, cited reference Schneier does not teach anything similar to the highlighted features but only reconstruction of a same secret by different persons wherein different numbers of persons belonging to different groups are able to reconstruct the secret. In other words, Schneier does **not** teach that persons belonging to group A can reconstruct portion A of the secret while persons belonging to group B can reconstruct portion B of the secret, which would be an equivalent to the feature defined in claim 6.

With respect to dependent claims 2 and 4, reference Matyas only teaches in col. 9 lines 11-14: "*To create a valid verification it is necessary that at least k of the users (where $0<k<n$) present valid biometric samples to the system.*", but not the feature defined in dependent claim 2.

Applicant respectfully submits that each of claims 2 and 4 depend on a claim that is believed to be allowable and as such are also allowable.

Dependent claim 3 has been canceled.

Claim 4 has been amended to replace the dependency on canceled claim 3 with the dependency on claim 2. No new subject matter has been added.

Claims Rejections – 35 USC § 103

Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Schneier, Applied Cryptography.

Applicant respectfully submits that claim 5 depends on a claim that is believed to be allowable and as such is also allowable.

Dependent claim 6 has been canceled.

Claims 7-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of references cited by Applicant.

Referring to amended independent claim 7, Applicant discloses and claims a method for providing access to a secure entity or service by M designated persons having only limited access privileges using a portable biometric device. The method comprises the same features as the method claimed in amended claim 1 and, in particular, the feature of: "*with $1 < N < M$ being a subset of a plurality of predetermined subsets of the M designated persons, wherein some of the subsets of the plurality of predetermined subsets have different access privileges to the secure entity or service*", which corresponds to the

highlighted features of claim 1.

As outlined above with respect to claim 1, the cited reference Matyas Jr. et al. is silent about such features. In particular, in col 9 lines 11-14 and lines 24-28, and in col. 10 lines 9-13, reference Matyas teaches only "*It is then determined if the count of valid users exceeds the threshold for authentication. ... If the threshold has been reached, then an indication of authenticity is provided.*" As is evident, the teachings of Matyas Jr. et al. enable access to the secure entity or service when the biometric information is indicative of a predetermined number of designated persons.

Reference Scott et al. has been cited by the applicant in paragraph [0012] of the disclosure as an example of a hand-held portable fingerprint recognition and transmission device.

Therefore, Applicant respectfully submits that it is not possible to obtain the method for providing access to a secure entity or service as defined in amended claim 7 by modifying the method of Matyas Jr. et al. to include the use of a portable biometric device.

No new subject matter has been added.

Applicant respectfully submits that each of claims 8 and 9 depend on a claim that is believed to be allowable and as such are also allowable.

Referring to amended claim 10 and dependent claim 13, Applicant discloses and claims a method for providing access to a secure entity or service by M designated persons having only limited access privileges comprising similar features as amended claims 1 and 7 and, in particular, the features as highlighted above with respect to amended claim 1. Claims 10 and 13 have been rejected for the same reasons as claim 7; therefore, the above arguments apply here mutatis mutandis.

No new subject matter has been added.

Referring to dependent claim 11, Applicant respectfully submits that cited reference

Matyas does not teach the feature of: "*determined access privileges define a time limitation*" but in col. 9 lines 38-53 timeout procedures or time durations in which received messages are considered for authorization. In other words, Matyas Jr. et al. teach preventing any access to a secure entity for certain time durations, **not** a time limitation for access to a specific predetermined subset of the designated persons. In the method defined in claim 11, the received biometric information is considered for authorization and in dependence upon determined access privileges – time limitations - for the predetermined subset access is denied or enabled. For example, one subset is enabled to access only during morning work hours while another subset is enabled to access only during afternoon work hours.

Referring to dependent claim 12, Applicant respectfully submits that cited reference Matyas teaches in col. 16 lines 42-49 only recovering of k shares of a key if k users are able to provide valid biometric information, **not** "*determined access privileges define functional limitations of the secure entity or service in dependence upon the subset of X persons*". This feature is highly beneficial by providing different levels of access to a secure entity or service for different subsets. For example, different subsets of different bank employees have access to different areas of a bank vault ensuring that only subsets of bank employees assigned to the tasks in a predefined section are able to access the same.

Applicant respectfully submits that each of claims 11 and 12 depend on a claim that is believed to be allowable and as such are also allowable.

Amended independent claim 14 defines a system for implementing the method for providing access to a secure entity or service as defined in amended claim 7 and has been rejected for the same reasons as claim 7; therefore, the above arguments apply here mutatis mutandis.

No new subject matter has been added.

Applicant respectfully submits that each of claims 15-17 depend on a claim that is

believed to be allowable and as such are also allowable.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of references cited by Applicant as applied to claim 17above, and further in view of Schneider et al. US Patent 5,456,256 .

Applicant respectfully submits that claim 18 depends on a claim that is believed to be allowable and as such is also allowable.

The prior art provided but not relied upon by the examiner has been reviewed. However, it is apparent that the references: Scott et al. (US Patent 6,111,977) and Scheidt et al. (US Patent 6,542,608) do not show anything similar to Applicant's invention as defined in the claims above.

Please charge any additional fees required or credit any overpayment to Deposit Account No. 50-1142.

Applicant requests favourable reconsideration of the amended application.

Respectfully,

Gordon Freedman, Reg. No. 41,553

Freedman and Associates
117 Centrepointe Drive, Suite 350
Nepean, Ontario
K2G 5X3 Canada

Tel (613) 274-7272
Fax (613) 274-7414

JF/sah